

EXHIBIT 92

**Redacted Version of
Document Sought to
be Sealed**

Incognito Mode, Current and Possible Promises

Author: rhalavati@

Status: WIP


Last Update: 2018-09-24

[go/incognito_promises](#)

Please see [go/incognito-mode](#) for the updated incognito definition.

Table of Contents

Incognito Mode, Current and Possible Promises	1
Table of Contents	1
Intro	2
Chrome Promises	2
Ephemeral State	3
User profile state should not change in incognito	3
No automatic scarification of privacy	3
Explicit warnings when privacy can't be guaranteed	3
Incognito mode and regular mode should not be linkable	4
Incognito mode should not be detectable	4
Default behavior of all features should respect incognito promises when called from incognito.	4
Enterprise Mode	4
User Expectations	5
Hide browsing history, especially visits to adult websites	5
Prevent targeted ads and search suggestions	5
Achieve "safer" browsing	5
Prevent browsers from saving login-related information	5
Avoid Cookies	6
Accommodate intentional or unintentional use by others.	6
Surfing Web Anonymously	6

Encrypted Communication with Websites	6
Hiding IP Address	6
Future Possibilities	7
	7
	7
	7
	7
	7
	7
	8
	8
Possible plans for future	8
	8
	9

Intro

This document discusses the current promises of incognito mode, user's expectations and understanding of them, and the ways to improve.

Related docs: [go/incognito-mode](#), [go/incognito-prd/](#)

Chrome Promises

As stated in incognito NTP, here are the general promises for incognito mode:

1. Chrome won't save your browsing history.
2. Chrome won't save your cookies and site data.
3. Chrome won't save your information entered in forms.

And it warns that the activity would still be visible to:

1. Websites¹.
2. Employer or school.
3. Internet service provider.

Internally we are trying to keep the following extended list of promises.

¹ But does not say the websites that talk to the websites that you navigate (3rd parties).

Ephemeral State

Unless there is a direct and clear user request, nothing should be stored on disk and if it is needed to do so, it should be encrypted while the key is kept in memory, and the data should be wiped on incognito mode close or next restart (in case of crash).

Downloads and saved files are examples of data that are stored by direct user action, browsing state in Android is a sample of encrypted on disk. Cookies have a separate jar that is cleared when incognito mode is closed.

User profile state should not change in incognito

No change in user preferences in incognito mode should affect regular mode. Exceptions of this rule are accessibility features, and bookmarks.

No automatic scarification of privacy

Any feature that disrespects privacy for a gain, should not be automatic in incognito and should be gated behind direct user action. Examples include:

- Autofill on incognito is not automatic and user needs selection of the suggested input to enter it.
- UKMs are disabled in incognito to avoid automatic data collection.
- Device identifiers or feature queries are completely behind user consent.
- All permissions are reduced towards factory default in incognito.
- Passing user information to other softwares is gated behind user consent or reduced.

Whenever possible, passing user information to OS should also be restricted in incognito. For example, notifications through OS UI should be stripped from user data in incognito as they might be logged by the OS.

Explicit warnings when privacy can't be guaranteed

Features that will affect the privacy of incognito mode should come with a clear warning, such as enabling extensions in incognito.

Incognito mode and regular mode should not be linkable

Any signature that can be used to connect the user's regular and incognito mode browsing should be avoided. This is to some extent violated by fingerprinting.

Incognito mode should not be detectable

We should not provide means for the websites to detect if the user is browsing in regular mode or incognito. To do so, all enabled features in incognito mode should seem similar to regular mode from a web facing point of view, and all disabled features, should be done so that it is done by the user. This is to some extent violated due to the missing features in incognito.

Default behavior of all features should respect incognito promises when called from incognito.

Privacy sensitive features should be implemented to respect incognito promises when run from incognito mode, and overriding them should need direct specification. E.g., preferences are saved in memory in incognito mode by default, and exceptional cases that need in profile storage are white listed to do so.

Enterprise Mode

Incognito mode should respect all the enforced policies. It would be good if Enterprise users would be warned that all specified policies are applied to the incognito mode as well and the promises are held in that context.

User Expectations

Based on Wu, et al.², and Habib et al.³, users use private browsing for the following expectations.

Comment [1]: +tnagel@google.com
Do we have any specific Enterprise promises?

Comment [2]: Afaiu the basic promise is that "enterprise policies don't apply" (e.g. extensions), but I'm not sure whether that's codified somewhere.

Comment [3]: I updated the text, please take a look.

Comment [4]: +mniissler@google.com Hey Mattias, do you have strong feelings about this? -- I'm not sure whether I do.

Comment [5]: This is tricky. Force-installed extension don't get access to incognito by default IIRC. All policy controls that are browser-global and not specific to a profile will affect incognito. Thus, I don't think there's a single valid policy on how enterprise management behaves for incognito, it's always been case-by-case decisions.

For Chrome OS, I don't feel too strongly - the OS user account is managed, so it's not surprising that incognito sessions within that user are subject to (some) management. On top of that, we have guest sessions as our solution for people who want an ephemeral browsing session with more guarantees.

On desktop, the situation is pretty complicated. If you're on a corp machine, it's similar to Chrome OS. What about BYOD though? With a corp-managed Chrome profile? I honestly don't know what the correct behavior for that case would be...

² "Your Secrets Are Safe: How Browsers' Explanations Impact Misconceptions About Private Browsing Mode", Wu et al., Proceedings of the 2018 World Wide Web Conference.

³ "Away From Prying Eyes: Analyzing Usage and Understanding of Private Browsing", Habib et al., Proceedings of the 14th Symposium on Usable Privacy and Security, Aug 2018, Baltimore, US.

Hide browsing history, especially visits to adult websites

If we consider hiding browsing history local, Incognito is completely doing that by clearing it after closing the current session. If it would be considered from network (ISP), or school, employer, etc., incognito is not doing so, and clearly has stated that it is not doing so.

Prevent targeted ads and search suggestions

This is done in incognito by separating the cookie jar and history in regular and incognito mode. We can consider it satisfied, but if a user stays long enough incognito mode and develop a new profile in incognito, this is not done.

Achieve “safer” browsing

Incognito mode is about privacy and not security. Not in the promises and not fulfilled.

Prevent browsers from saving login-related information

Similar to targeted ads, this is completely done by separating the cookie jars, but not in one incognito session.

Avoid Cookies

Like above item. Maybe we should know why users want cookieless browsing. Does that mean 3rd party cookies and avoiding targeted ads, or some other functionality is desired.

Accommodate intentional or unintentional use by others.

Partly done by not altering user profile or history in incognito mode, but better to be done in guest mode.

Surfing Web Anonymously

Anonymous surfing is partly done by creating a fresh profile on each entry of the incognito mode. But fingerprinting to some extent disrupts the total clean slate, and maybe, users expect no trace from an inside one incognito session experience, which can be a cookie-siloed browsing.

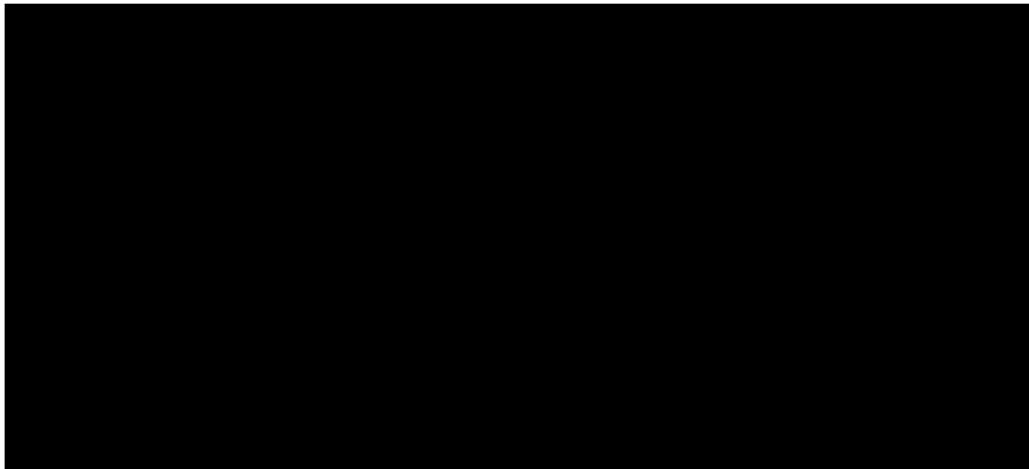
Encrypted Communication with Websites

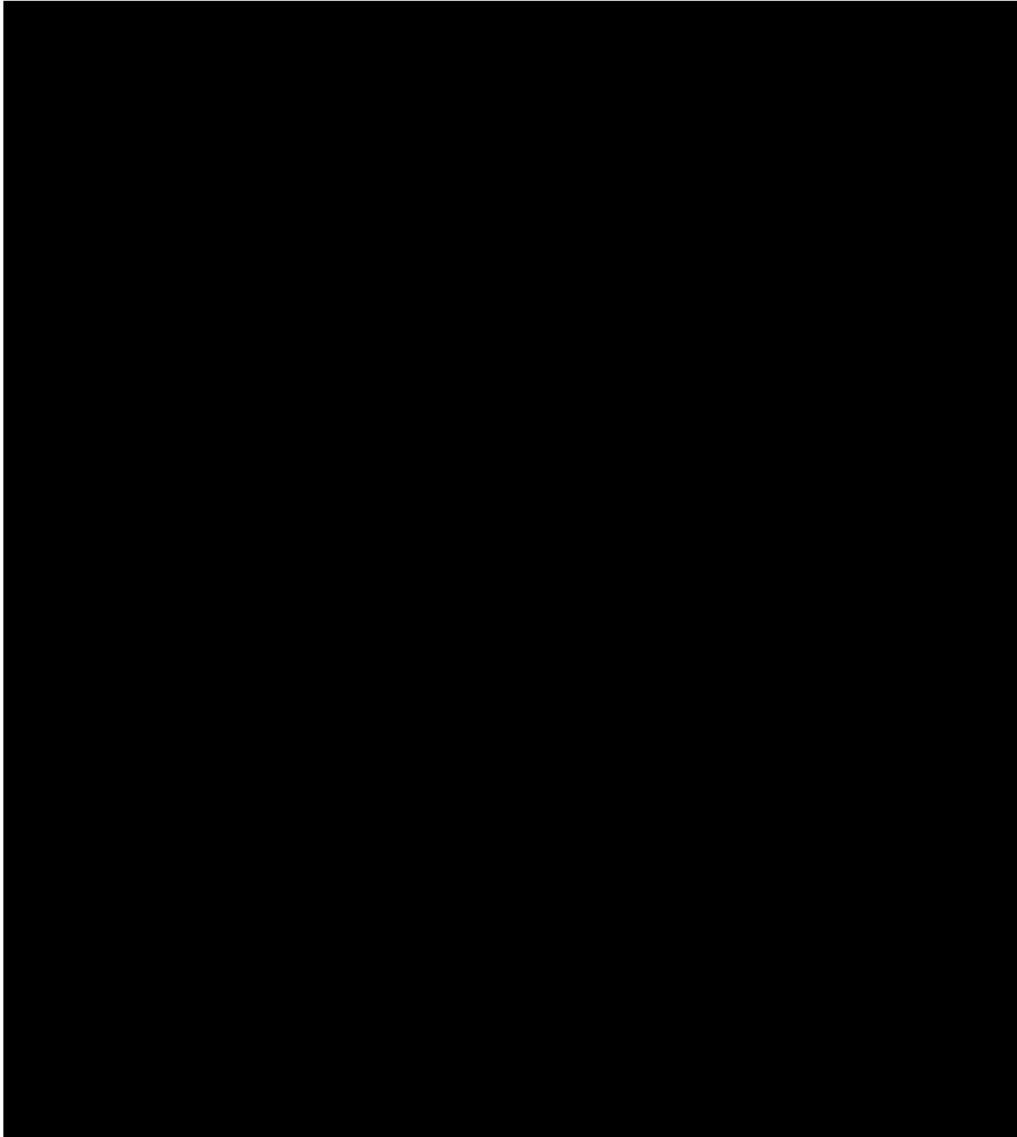
Incognito mode does not enforce HTTPS, or even upgrade by default if it's safe.

Hiding IP Address

Not covered.

Future Possibilities





Possible plans for future

